



⑯ BUNDESREPUBLIK  
DEUTSCHLAND



**DEUTSCHES  
PATENT- UND  
MARKENAMT**

⑫ **Offenlegungsschrift**  
⑩ **DE 199 24 575 A 1**

⑤ Int. Cl.<sup>6</sup>:  
**H 04 L 29/06**  
H 04 L 12/22  
G 06 F 13/00  
G 06 F 12/14  
// H04L 9/00

21 Aktenzeichen: 199 24 575.4  
22 Anmeldetag: 28. 5. 99  
43 Offenlegungstag: 2. 12. 99

⑩ Unionspriorität:  
087823 29. 05. 98 US

⑪ Anmelder:  
Sun Microsystems, Inc., Palo Alto, Calif., US

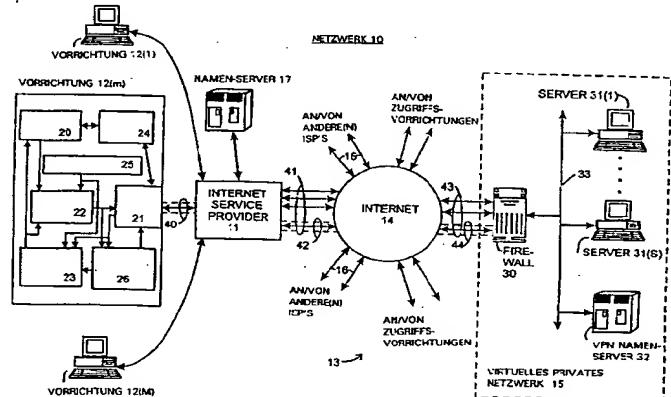
⑫ Vertreter:  
Samson & Partner, Patentanwälte, 80538 München

72 Erfinder:  
Provino, Joseph E., Cambridge, Mass., US

**Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen**

## ⑤4 Kommunikationssystem und -Verfahren

57) Das erfundungsgemäße System umfaßt ein virtuelles privates Netzwerk (15) und eine externe Vorrichtung (12(m)), welche durch ein digitales Netzwerk (14) miteinander verbunden sind. Das virtuelle private Netzwerk (15) weist eine Firewall (30), wenigstens eine interne Vorrichtung (31(s)) und einen Namen-Server (32) auf, welche jeweils eine Netzwerkadresse besitzen. Die interne Vorrichtung (31(s)) besitzt auch eine Sekundäradresse, und der Namen-Server (32) ist derart konfiguriert, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt. In Reaktion auf eine Anfrage von der externen Vorrichtung (12(m)) zum Aufbau einer Verbindung zur Firewall (30) übermittelt die Firewall (30) der externen Vorrichtung (12(m)) die Netzwerkadresse des Namen-Servers (32). In Reaktion auf eine Anfrage von einem Bediener oder ähnlichem, welche die Sekundäradresse der internen Vorrichtung (31(s)) enthält und einen Zugriff an die interne Vorrichtung (31(s)) anfordert, erzeugt die externe Vorrichtung (12(m)) eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (30), welche eine Auflösung der Netzwerkadresse, die der Sekundäradresse zugeordnet ist, anfordert. Die Firewall (30) übermittelt die Adressenauflösungsanfrage an den Namen-Server (32), und der Namen-Server (32) übermittelt die Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, an die Firewall (30). Daraufhin stellt die Firewall (30) die Netzwerkadresse in einer ...



## Beschreibung

Die Erfindung betrifft allgemein das Gebiet der digitalen Kommunikationssysteme und -verfahren, und insbesondere Systeme und Verfahren zum Vereinfachen der Kommunikation zwischen Vorrichtungen, welche mit öffentlichen Netzwerken verbunden sind, z. B. dem Internet, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind.

Digitale Netzwerke wurden entwickelt, um die Übertragung von Information, welche auch Daten und Programme umfaßt, über digitale Computersysteme und andere Digitalvorrichtungen zu ermöglichen. Es wurde eine Vielzahl von Arten von Netzwerken entwickelt und realisiert, einschließlich sog. Fernverbindungsnetze (Wide-Area Networks, nachfolgend "WAN" genannt) und lokale Netzwerke (Local Area Networks, nachfolgend "LAN" genannt), welche eine Information unter Verwendung verschiedener Informationsübertragungsmethoden übermitteln. Im allgemeinen werden LANs innerhalb kleiner geographischer Bereiche realisiert, z. B. innerhalb eines einzelnen Bürogebäudes oder ähnlichem, zum Übertragen von Information innerhalb eines bestimmten Büros, einer Firma oder einer ähnlichen Art von Organisationseinheit. Andererseits werden WANs im allgemeinen auf relativ großen geographischen Bereichen realisiert und können verwendet werden, um Information sowohl zwischen LANs als auch zwischen Vorrichtungen, welche nicht mit LANs verbunden sind, zu übertragen. Derartige WANs umfassen auch öffentliche Netzwerke, z. B. das Internet, welche zur Informationsübertragung zwischen einer Anzahl von Unternehmen verwendet werden können.

Es sind mehrere Probleme im Zusammenhang der Kommunikation über ein Netzwerk aufgetreten, insbesondere in einem großen öffentlichen WAN, wie es z. B. das Internet ist. Im allgemeinen werden Informationen über ein Netzwerk in Nachrichtenpaketen übertragen, welche ausgehend von einer Vorrichtung, als Quelle bzw. Quellenvorrichtung, zu einer anderen Vorrichtung, als Ziel bzw. Zielvorrichtung, über einen oder mehrere Router oder allgemein Schaltungsknoten im Netzwerk übertragen werden. Jedes Nachrichtenpaket enthält eine Zieladresse, welche von den Schaltungsknoten verwendet wird, um das jeweilige Nachrichtenpaket an die geeignete Zielvorrichtung zu leiten. Z.B. im Internet haben solche Adressen die Form von "n"-Bit Zahlen (wobei "n" 32 oder 128 sein kann), wobei solche Zahlenkolonnen für einen Benutzer schwierig sind zu merken und einzugeben, wenn die oder der Benutzer die Übertragung eines Nachrichtenpaketes veranlassen möchte. Um einen Benutzer von der Notwendigkeit zu befreien, sich solche spezifische Zahlen-Internetadressen zu merken und einzugeben, stellt das Internet einen zweiten Adressierungsmechanismus bereit, der durch Benutzer der jeweiligen Vorrichtungen einfacher handzuhaben ist. Bei diesem Adressierungsmechanismus werden Internet-Domains, wie etwa LANs, Internet-Service-Provider (nachfolgend "ISP" genannt) und ähnliche, welche im Internet verbunden sind, durch für einen Benutzer relativ einfach les- und merkbare Namen identifiziert, die nachfolgend als "Klartextnamen" bezeichnet werden. Um den Einsatz von solchen Klartextnamen umzusetzen, werden Namen-Server, auch als DNS-Server für "Domain Name Server" bezeichnet, bereitgestellt, um die Klartextnamen in die geeigneten Internetadressen umzuwandeln. Wenn ein Benutzer einer Vorrichtung, der die Übertragung eines Nachrichtenpaketes an eine andere Vorrichtung wünscht, den Klartextnamen der anderen Vorrichtung eingibt, nimmt die Vorrichtung zuerst Kontakt mit einem Namen-Server auf. Im allgemeinen kann der Namen-Server ein Teil des ISP selbst sein oder er kann eine spezielle Vorrichtung sein, welche durch den ISP über das Internet zugäng-

lich ist; in jedem Fall wird der ISP den Namen-Server identifizieren, welcher für die Vorrichtung zu verwenden ist, wenn sich die Vorrichtung beim ISP einloggt, d. h. anmeldet. Falls der Namen-Server, nachdem die Vorrichtung einen

- 5 Kontakt hergestellt hat, eine Zahlen-Internetadresse für den Klartext-Domainnamen besitzt oder erhalten kann, übermittelt der Namen-Server die Zahlen-Internetadresse, welche dem Klartext-Domainnamen entspricht, zu der Vorrichtung des Bedieners. Die Vorrichtung kann sodann die Zahlen-Internetadresse, welche von dem Namen-Server zurückgesendet wurde, in das Nachrichtenpaket einfügen und das Nachrichtenpaket an den ISP für die Übertragung über das Internet auf konventioneller Weise liefern. Die Internet-Schaltungsknoten verwenden die Zahlen-Internetadresse, um das Nachrichtenpaket an die gewünschte Zielvorrichtung zu übermitteln.

Andere Probleme treten insbesondere in Verbindung mit der Übertragung von Information über ein öffentliches WAN, z. B. das Internet, auf. Ein Problem besteht darin, sicherzustellen, daß die über das WAN übertragene Information, welche die Quellenvorrichtung und die Zielvorrichtung vertraulich behalten möchten, auch tatsächlich vertraulich bleibt gegenüber möglichen Lauschern, welche die Information abfangen können. Um die Vertraulichkeit zu wahren, 20 wurden verschiedene Formen von Verschlüsselung entwickelt und werden verwendet, um die Information vor der Übertragung durch die Quellenvorrichtung zu verschlüsseln und die Information nach deren Empfang durch die Zielvorrichtung zu entschlüsseln. Falls gewünscht wird, daß beispielweise die gesamte Information, welche zwischen einer bestimmten Quellenvorrichtung und einer bestimmten Zielvorrichtung übertragen wird, vertraulich bleiben soll, können die Vorrichtungen einen sog. "Sicherheitstunnel" zwischen den Vorrichtungen einrichten, der im wesentlichen sicherstellt, daß die gesamte Information, welche von der Quellenvorrichtung an die Zielvorrichtung übertragen wird, vor der Übertragung verschlüsselt wird (mit Ausnahme von bestimmten Protokollinformationen, wie Adresseninformation, welche den Fluß von Netzpaketen über das Netzwerk 30 zwischen der Quellen- und Zielvorrichtung steuert), und daß die verschlüsselte Information vor der Verwendung durch die Zielvorrichtung entschlüsselt wird. Die Quellen- und Zielvorrichtungen können jeweils für sich eine Verschlüsselung bzw. Entschlüsselung durchführen, oder die Verschlüsselung und Entschlüsselung kann durch andere Vorrichtungen durchgeführt werden, bevor die Nachrichtenpakete über 40 das Internet übertragen werden.

Ein weiteres Problem, welches insbesondere im Zusammenhang mit Unternehmen, Regierungsämtern und privaten Organisationen auftritt, deren private Netzwerke, welche LANs, WANs oder etwaige Kombinationen derselben sein können, mit öffentlichen WANs, z. B. dem Internet, verbunden sind, besteht darin, sicherzustellen, daß deren private Netzwerke sicher sind gegenüber anderen Netzwerken, zu welchen z. B. die Unternehmen keinen Zugriff haben möchten, oder einen Zugriff durch andere zu regulieren und zu kontrollieren, zu welchen z. B. die jeweiligen Organisationen einen begrenzten Zugriff haben möchten. Um dies umzusetzen, verbinden die Organisationen in der Regel ihre privaten Netzwerke mit öffentlichen WANs über eine begrenzte Anzahl von Gateways, welche manchmal als "Firewalls" bezeichnet werden, durch welche der gesamte Netzverkehr zwischen dem internen und dem öffentlichen Netzwerk läuft. In der Regel sind Netzwerkadressen von Domains und Vorrichtungen in dem privaten Netzwerk "hinter" der Firewall den Namen-Servern bekannt, welche in den privaten Netzwerken vorgesehen sind; sie sind aber nicht zugänglich für Namen-Server oder andere Vorrichtungen au-

Berhalb der privaten Netzwerke, was die Kommunikation zwischen einer Vorrichtung außerhalb des privaten Netzwerkes und einer Vorrichtung innerhalb des privaten Netzwerkes schwierig macht.

Ein Ziel der vorliegend Erfindung ist es, hier Abhilfe zu schaffen.

Dieses Ziel erreicht die Erfindung durch die Gegenstände der Ansprüche 1, 7 und 13. Bevorzugte Ausführungsbeispiele der Erfindung sind in den jeweils abhängigen Ansprüchen beschrieben.

Danach schafft die Erfindung ein neuartiges und verbessertes System und ein Verfahren zum Vereinfachen von Kommunikation zwischen Vorrichtungen, welche mit öffentlichen Netzwerken, z. B. dem Internet, verbunden sind, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind, wobei die Auflösung von Sekundäradressen, wie etwa Text- bzw. Klartextnamen im Internet, in die zugehörigen Netzwerkadressen durch Namen-Server oder ähnliche Vorrichtungen, die mit den privaten Netzwerken verbunden sind, ermöglicht wird.

Hierfür stellt die Erfindung ein System zur Verfügung mit einem virtuellen Privaten Netzwerk und einer externen Vorrichtung, welche durch ein digitales Netzwerk miteinander verbunden sind, sowie ein Kommunikationsverfahren und ein Computerprogrammprodukt zum gemeinsamen Verwenden mit einem derartiges System. Das virtuelle private Netzwerk weist eine Firewall bzw. ein Firewall-System, wenigstens eine interne Vorrichtung und einen Namen-Server auf, welche jeweils eine Netzwerkadresse besitzen. Die interne Vorrichtung besitzt ferner eine Sekundäradresse, und der Namen-Server ist derart konfiguriert, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt. In Reaktion auf eine Anfrage von der externen Vorrichtung zum Aufbau einer Verbindung zur Firewall übermittelt die Firewall der externen Vorrichtung die Netzwerkadresse des Namen-Servers. In Reaktion auf eine Anfrage von einem Bediener oder ähnlichem, welche die Sekundäradresse der internen Vorrichtung enthält und einen Zugriff an die interne Vorrichtung anfordert, erzeugt die externe Vorrichtung eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall, welche eine Auflösung der Netzwerkadresse, die der Sekundäradresse zugeordnet ist, anfordert. Die Firewall übermittelt die Adressenauflösungsanfrage an den Namen-Server und der Namen-Server übermittelt die Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, an die Firewall. Daraufhin stellt die Firewall die Netzwerkadresse in einer Netzwerkadressenantwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung bereit. Die externe Vorrichtung kann sodann die auf diese Weise bereitgestellte Netzwerkadresse in nachfolgenden an die interne Vorrichtung gerichtete Kommunikationen mit der Firewall verwenden.

Weitere Vorteile und Ausgestaltungen der Erfindung ergeben sich aus der nachfolgenden detaillierten Beschreibung eines bevorzugten Ausführungsbeispiels. In der Beschreibung wird auf die beigelegte schematische Zeichnung Bezug genommen. Darin zeigt:

Fig. 1 ein funktionelles Blockdiagramm eines erfindungsgemäßen Netzwerkes.

Fig. 1 zeigt ein funktionelles Blockdiagramm eines Netzwerkes 10, welches gemäß der vorliegenden Erfindung aufgebaut ist. Das Netzwerk 10 gemäß Fig. 1 umfaßt einen Internet-Service-Provider (nachfolgend "ISP") 11, welcher die Übertragung von Nachrichtenpaketen zwischen einer oder mehreren Vorrichtungen 12(1) bis 12(M) (nachfolgend allgemeinen mit dem Bezugszeichen 12(m) identifiziert), welche mit dem ISP 11 verbunden sind, und anderen Vorrich-

tungen, welche allgemein durch ein Bezugszeichen 13 gekennzeichnet sind, über das Internet 14 ermöglicht, wobei die Übertragung von Information in Nachrichtenpaketen zwischen den Vorrichtungen 12(m) und 13 realisiert wird.

- 5 5 Der ISP 11 verbindet das Internet 14 über eine oder mehrere logische Verbindungen oder Gateways oder ähnlichem (im vorliegenden allgemein als "Verbindungen" bezeichnet), welche allgemein durch das Bezugszeichen 41 gekennzeichnet sind. Der ISP 11 kann ein öffentlicher ISP sein, welcher in diesem Falle die Verbindung mit Vorrichtungen 12(n) herstellt, welche durch Bediener betrieben werden können, die der allgemeinen Öffentlichkeit angehören, so daß diese Bediener Zugang zu dem Internet erlangen. Alternativ dazu kann der ISP 11 ein privater ISP sein. In diesem Falle werden die damit verbundenen Vorrichtungen 12(m) im allgemeinen beispielsweise durch Angestellte eines bestimmten Unternehmens oder einer Regierungseinrichtung, Mitgliedern von einer privaten Organisation oder ähnlichen betrieben, um diesen Angestellten oder Mitglieder einen Zugang 15 in das Internet bereit zu stellen.

In an sich konventioneller Weise weist das Internet ein Netz von Schaltungsknoten auf (welche nicht separat dargestellt sind), welche die ISPs 11 und die Vorrichtungen 13 miteinander verbinden, um dazwischen die Übertragung 25 von Nachrichtenpaketen zu ermöglichen. Die Nachrichtenpakete, welche über das Internet 14 übertragen werden, stimmen mit denjenigen überein, welche durch das sog. Internetprotokoll (IP) definiert werden, und umfassen einen Kopfabschnitt, einen Datenabschnitt und können einen Fehlerfassungs- und/oder Korrekturabschnitt aufweisen. Der Kopfabschnitt enthält Information, welche verwendet wird, um das Nachrichtenpaket über das Internet 14 zu übertragen, beispielsweise eine Zieladresse, welche die Vorrichtung identifiziert, welche das Nachrichtenpaket als Zielvorrichtung empfangen soll, und eine Quellenadresse, welche diejenige Vorrichtung identifiziert, welche das Nachrichtenpaket erzeugt hat. In jedem Nachrichtenpaket haben die Ziel- und Quellenadresse jeweils die Form einer Zahl, welche eindeutig die jeweilige Ziel- bzw. Quellenvorrichtung 35 identifiziert. Die Schaltungsknoten im Internet 14 verwenden wenigstens die Zieladresse eines jeweiligen Nachrichtenpaketes, um das jeweilige Nachrichtenpaket an die Zielvorrichtung zu übermitteln, wenn die Zielvorrichtung an das Internet angeschlossen ist, oder an einen ISP 11 oder andere Vorrichtungen, welche an das Internet 14 angeschlossen sind, welche sodann das Nachrichtenpaket an das geeignete Ziel senden werden. Der Datenabschnitt eines jeden Nachrichtenpakets enthält die in dem Nachrichtenpaket übertragenen Daten; und der Fehlerfassungs- und/oder Korrekturabschnitt enthält Fehlerfassungs- und/oder Korrekturinformationen, welche verwendet werden können, um zu verifizieren, daß das Nachrichtenpaket in korrekter Weise von der Quelle zu der Zielvorrichtung übertragen wurde (im Fall der Fehlerfassungsinformation), und um ausgewählte 45 Arten von Fehlern zu korrigieren, falls das Nachrichtenpaket nicht korrekt übertragen wurde (im Falle der Fehlerkorrekturinformation).

Die Vorrichtungen 12(m), welche mit dem ISP 11 verbunden sind, können jede beliebige Anzahl von Arten von Vorrichtungen umfassen, welche über das Internet 14 mit anderen Vorrichtungen 13 kommunizieren, umfassend z. B. Personalcomputer, Computer-Workstations und ähnliches. Jede Vorrichtung 12(m) kommuniziert mit dem ISP 11, um Nachrichtenpakete für die Übertragung über das Internet 14 an diesen zu übertragen, oder um Nachrichtenpakete, welche durch den ISP 11 über das Internet empfangen werden, von diesem zu empfangen. Dabei kann jedes geeignete Protokoll verwendet werden, z. B. das bekannte Point-to-Point Proto-

koll (allgemein mit "PPP" abgekürzt), falls die Vorrichtung 12(m) über eine Point-to-Point Verbindung mit dem ISP 11 verbunden ist, oder irgendein konventionelles "Multi-Drop" Protokoll, falls die Vorrichtung 12(m) mit dem ISP 11 über ein "Multi-Drop"-Netzwerk, z. B. das Ethernet, verbunden ist, oder ähnliches. Die Vorrichtungen 12(m) sind im allgemeinen entsprechend der üblichen Computerarchitektur mit gespeicherten Programmen aufgebaut, welche z. B. eine Systemeinheit, eine Bildschirmanzeigeeinheit und Bedienereingabeeinrichtungen, wie etwa eine Tastatur oder eine Maus, umfaßt. Eine Systemeinheit weist im allgemeinen eine oder mehrere Prozessor-, Speicher-, Massenspeicher- einrichtungen, z. B. Festplatten- und/oder Bandspeicherelemente, oder andere Elemente (nicht separat gezeigt) auf, wie etwa Netzwerk- und/oder Telefonschnittstelleneinrichtungen, um die jeweilige Vorrichtung an den ISP 11 anzukopeln. Die Prozessor- bzw. Verarbeitungseinrichtungen verarbeiten Programme, einschließlich Anwendungsprogramme, unter der Steuerung eines Betriebssystems, um verarbeitete Daten zu erzeugen. Die Bildschirmeinheit ermöglicht es der Vorrichtung, die verarbeiteten Daten und einen Verarbeitungsstatus der Daten dem Benutzer anzuzeigen, und die Bedienereingabeeinrichtung ermöglicht es dem Bediener, Daten einzugeben und die Verarbeitung zu steuern.

Diese Elemente der Vorrichtung 12(m) arbeiten in Verbindung mit einer geeigneten Programmierung so zusammen, um eine Vorrichtung 12(m) mit einer Anzahl von funktionellen Elementen bereit zu stellen, beispielsweise eine Bedienerchnittstelle 20, eine Netzwerkschnittstelle 21, einen Nachrichtenpaketgenerator 22, einen Nachrichtenpaketempfänger und -prozessor 23, eine ISP Einloggsteuerung bzw. Anmeldungssteuerung 24, einen Internetparameterspeicher 25 und im Zusammenhang mit der vorliegenden Erfindung einen Sicherheits-Nachrichtenpaketprozessor 26. Die Bedienerchnittstelle 20 ermöglicht, daß die Vorrichtung 12(m) Eingabeinformationen von der/den Bedienereingabeevorrichtung(en) der Vorrichtung 12(m) empfängt und die Ausgabeinformationen dem Bediener auf der/den Bildschirmeinrichtung(en) der Vorrichtung 12(m) angezeigt werden. Die Netzwerkschnittstelle 21 ermöglicht eine Verbindung der Vorrichtung 12(m) mit dem ISP 11 unter Verwendung des geeigneten PPP oder Netzwerkprotokolls, um Nachrichtenpakete an den ISP 11 zu übertragen und von diesem Nachrichtenpakete zu empfangen. Die Netzwerkschnittstelle 21 kann eine Verbindung mit dem ISP 11 über das öffentliche Telefonnetz vorsehen, um einen Wählverbundungsnetzwerkbetrieb (sog. Dial-Up Betrieb) der Vorrichtung 12(m) über das öffentliche Telefonnetz zu ermöglichen. Alternativ oder zusätzlich dazu kann die Netzwerkschnittstelle 21 eine Verbindung durch den ISP 11 über beispielsweise ein konventionelles LAN ermöglichen, wie etwa das Ethernet. In Reaktion auf eine durch die Bedienerchnittstelle 20 gelieferte Eingabe und/oder in Reaktion auf Anfragen aus Programmen (nicht gezeigt), welche durch die Vorrichtung 12(m) verarbeitet werden, kommuniziert die ISP Einloggsteuerung 24 über die Netzwerkschnittstelle 21, um die Initialisierung (sog. "Log-On") einer Kommunikationszusammenstellung zwischen der Vorrichtung 12(m) und dem ISP 11 zu ermöglichen. Während dieser Kommunikationszusammenstellung kann die Vorrichtung 12(m) Information in der Form von Nachrichtenpaketen an andere Vorrichtungen über das Internet 14 sowie an andere Vorrichtungen 12(m') (wobei  $m' \neq m$ ), welche mit der ISP 11 oder mit anderen ISPs verbunden sind, übertragen. Während eines Log-On-Betriebs empfängt die ISP Einloggsteuerung 24 die Internetprotokollparameter (IP-Parameter), welche im Zusammenhang mit einer Nachrichtenpaketzeugung während der Kommunikationszusammenstellung verwendet werden.

Während einer Kommunikationszusammenstellung erzeugt der Nachrichtenpaketgenerator 22 Nachrichtenpakete zur Übertragung durch die Netzwerkschnittstelle 21 in Reaktion auf eine Eingabe, welche durch den Bediener über die Bediener- 5 schnittstelle 20 geliefert wird und/oder in Reaktion auf Anfragen aus Programmen (nicht separat gezeigt), welche durch die Vorrichtung 12(m) verarbeitet werden. Die Netzwerkschnittstelle 21 empfängt auch Nachrichtenpakete aus dem ISP 11 und liefert diese an den Nachrichtenpaketempfänger und -prozessor 23 zur Verarbeitung und Bereitstellung an die Bedienerchnittstelle 20 und/oder anderen Programmen (nicht gezeigt), welche durch die Vorrichtung 12(m) verarbeitet werden. Falls die empfangenen Nachrichtenpakete eine Information enthalten, z. B. Web-Seiten oder ähnliches, welche dem Bediener angezeigt werden soll, kann die Information der Bedienerchnittstelle 20 geliefert werden, damit die Information auf der Bildschirmeinheit der Vorrichtung angezeigt wird. Zusätzlich oder alternativ dazu kann die Information an andere Programme (nicht gezeigt) zur Verarbeitung geliefert werden, welche durch die Vorrichtung 12(m) verarbeitet werden.

Im allgemeinen können die Elemente, wie die Bediener- 10 schnittstelle 20, der Nachrichtenpaketgenerator 22, der Nachrichtenpaketempfänger und -prozessor 23, die ISP Einloggsteuerung 24 und der Internetparameterspeicher 25 Elemente eines konventionellen Internet-Browsers enthalten, wie die von Mosaic, Netscape Navigator und Microsoft Internet Explorer.

Wie es oben erwähnt wurde, weist die Vorrichtung 12(m) 15 im Zusammenhang mit der vorliegenden Erfindung einen Sicherheits-Nachrichtenpaketprozessor 26 auf. Der Sicherheits-Nachrichtenpaketprozessor 26 ermöglicht den Aufbau und Verwendung eines "Sicherheitstunnels" zwischen der Vorrichtung 12(m) und anderen Vorrichtungen 12(m') (wobei  $m' \neq m$ ) oder 13, wie es weiter unten beschrieben wird. Im allgemeinen wird in einem solchen Sicherheitstunnel Information in wenigstens dem Datenabschnitt der zwischen der Vorrichtung 12(m) und einer spezifischen anderen Vorrichtung 12(m') (wobei  $m' \neq m$ ) oder 13 übertragenen Nachrichtenpakete geheimgehalten, beispielsweise durch Verschlüsselung des Datenabschnittes vor der Übertragung durch die Quellenvorrichtung. Die Information in anderen Abschnitten eines derartigen Nachrichtenpakets kann ebenfalls geheimgehalten werden, mit Ausnahme der 20 Information, welche benötigt wird, um die Übertragung des jeweiligen Nachrichtenpaketes zwischen den Vorrichtungen zu ermöglichen, also z. B. wenigstens die Zielerinformation, damit die Schaltungsknoten des Internets und die ISPs die Vorrichtung identifizieren können, welche das Nachrichtenpaket 25 empfangen soll.

Zusätzlich zu dem ISP 11 kann eine Vielzahl von anderen ISPs die Verbindung zum Internet herstellen, wie es durch die Pfeile 16 angedeutet ist, um eine Kommunikation zwischen Vorrichtungen, welche an diesen anderen ISPs angeschlossen sind, mit anderen Vorrichtungen über das Internet zu ermöglichen, welche die Vorrichtungen 12(n), welche an dem ISP 11 angeschlossen sind, umfassen können.

Die Vorrichtungen 13, auf welche die Vorrichtungen 12(m) zugreifen und mit welchen diese kommunizieren, 30 können auch von jeder beliebigen Anzahl von Arten von Vorrichtungen sein, einschließlich Personalcomputer, Computer-Workstations und ähnliches, oder auch Minicomputer und Großrechner, Großspeichersysteme, Rechenserver, lokale Netzwerke (LANs) und Fernverbindungsnetzwerke (WANs), welche derartige Vorrichtungen und zahlreiche andere Arten von Vorrichtungen enthalten, die direkt oder indirekt mit den Netzwerken verbunden werden können. Nach 35 den vorliegenden Erfindungen umfaßt wenigstens eine der Vor-

richtungen wenigstens ein privates Netzwerk, welches als virtuelles privates Netzwerk 15 gekennzeichnet ist und z. B. die Form eines LAN oder eines WAN haben kann. Das virtuelle private Netzwerk 15 kann jede der Vorrichtungen 12(m') (wobei  $m' \neq m$ ) aufweisen (wobei die Verbindung zu dem Internet 14 über einen ISP erfolgt) oder der Vorrichtungen 13 (wobei die Verbindung zu dem Internet 14 unmittelbar erfolgt). Bei dem vorliegend beschriebenen Ausführungsbeispiel wird angenommen, daß das virtuelle Netzwerk 15 eine Vorrichtung 13 aufweist. Das virtuelle private Netzwerk 15 umfaßt selbst mehrere Vorrichtungen, welche hier als eine Firewall bzw. ein Firewall-System 30, mehrere Server 31(1) bis 31(S) (im nachfolgenden allgemein mit dem Bezeichnungen 31(s) angegeben) und ein Namen-Server 32 gekennzeichnet sind, wobei allesamt durch eine Übertragungsverbindung 33 miteinander verbunden sind. Die Firewall 30 und die Server 31(s) können ähnlich sein wie jede der verschiedenen Arten von Vorrichtungen 12(m) und 13, die hier beschrieben sind, und können daher beispielsweise umfassen Personalcomputer, Computer-Workstations und ähnliches, aber auch Minicomputer und Großrechner, Großspeichersysteme, Rechenserver, lokale Netzwerke (LANs) und Fernverbindungsnetzwerke (WANs), welche derartige Vorrichtungen und zahlreiche andere Arten von Vorrichtungen umfassen, welche direkt oder indirekt mit den Netzwerken verbunden werden können.

Wie oben ausgeführt wurde, kommunizieren diese Vorrichtungen einschließlich der Vorrichtungen 12(m) und der Vorrichtungen 13 durch Übertragung von Nachrichtenpaketen über das Internet. Die Vorrichtungen 12(m) und 13 können Information in einem Peer-to-Peer bzw. gleichrangigem Modus, in einem Client-Server Modus oder nach beiden dieser Modi übertragen. Im allgemeinen überträgt eine Vorrichtung in einer Peer-to-Peer Nachrichtenpaketübertragung Information in einem oder mehreren Nachrichtenpaketen an die andere Vorrichtung. Andererseits kann eine Vorrichtung, welche in einem Client-Server Modus als Client fungiert, ein Nachrichtenpaket an eine andere Vorrichtung übertragen, welche als Server fungiert, um beispielsweise einen Dienst durch die andere Vorrichtung auszulösen. Mehrere Arten derartiger Dienste sind dem Fachmann bekannt, beispielsweise das Wiedergewinnen bzw. Auslesen von Information aus der anderen Vorrichtung, damit diese aktiviert wird, um Verarbeitungsoperationen und dergleichen durchzuführen. Falls der Server dazu dient, dem Client vor allem Informationen zu liefern, kann dieser allgemein als ein Speicherserver bezeichnet werden. Falls der Server andererseits Verarbeitungsoperationen auf Anfrage des Client ausführen soll, kann dieser allgemein als ein Rechenserver bezeichnet werden. Andere Arten von Servern zum Ausführen von anderen Arten von Diensten und Operationen auf Anfrage von Clients sind dem Fachmann ebenfalls bekannt.

Wenn in einer Client-Server Anordnung eine Vorrichtung 12(m) einen Dienst durch beispielsweise eine Vorrichtung 13 ausgeführt haben möchte, erzeugt die Vorrichtung 12(m) eines oder mehrere Anfragenachrichtenpakete zur Übertragung an die Vorrichtung 13, welche den benötigten Dienst anfordern. Das Anfragenachrichtenpaket enthält die Internetadresse der Vorrichtung 13, welche als die Zielvorrichtung das Nachrichtenpaket empfängt und den Dienst ausführt. Die Vorrichtung 12(m) überträgt das/die Anfragenachrichtenpaket(e) an den ISP 11. Der ISP 11 überträgt daraufhin das Nachrichtenpaket über das Internet an die Vorrichtung 13.

Falls die Vorrichtung 13 die Form eines WAN oder LAN hat, empfängt das WAN oder LAN das/die Nachrichtenpaket(e) und leitet dieses/diese zu einer dort angeschlossenen Vorrichtung weiter, welche den angeforderten Dienst aus-

führen soll.

In jedem Fall wird die Vorrichtung 13, welche den angeforderten Dienst ausführen soll, nach Empfang des/der Anfragenachrichtenpaket(e) die Anfrage bearbeiten. Falls die 5 Vorrichtung 12(m), welche das/die Anfragenachrichtenpaket(e) erzeugt hat, oder deren Bediener die notwendigen Befugnisse hat, um den Dienst von der Vorrichtung 13 anzufordern, und falls der angeforderte Dienst die Einleitung einer Informationsübertragung aus der Vorrichtung 13 als ein 10 Speicherserver an die Vorrichtung 12(m) als ein Client umfaßt, erzeugt die Vorrichtung 13 eines oder mehrere Antwortnachrichtenpakete, welche die angeforderten Information enthalten, und überträgt das/die Paket(e) über das Internet 14 an den ISP 11. Daraufhin überträgt der ISP 11 das/die 15 Nachrichtenpaket(e) an die Vorrichtung 12(m). Falls andererseits der angeforderte Dienst die Einleitung eines Verarbeitungsvorganges durch die Vorrichtung 13 als ein Rechenserver beinhaltet, wird die Vorrichtung 13 den/die angeforderten Rechendienst(e) ausführen. Falls die Vorrichtung 13 20 verarbeitete Daten, welche während den Rechenvorgängen erzeugt wurden, an die Vorrichtung 12(m) als Client zurücksenden soll, erzeugt die Vorrichtung 13 zusätzlich eines oder mehrere Antwortnachrichtenpakete, welche die verarbeiteten Daten enthalten und überträgt das/die Paket(e) über das 25 Internet 14 an den ISP 11. Der ISP 11 überträgt daraufhin das/die Nachrichtenpaket(e) an die Vorrichtung 12(m). Entsprechende Operationen können durch die Vorrichtungen 12(m) und 13, dem ISP 11 und dem Internet 14 in Verbindung mit anderen Arten von Diensten ausgeführt werden, 30 welche durch die Server-Vorrichtungen 13 bereitgestellt werden können.

Wie oben angemerkt wurde, enthält jedes Nachrichtenpaket, welches durch die Vorrichtungen 12(m) und 13 zur Übertragung über das Internet 14 erzeugt wird, eine Zieladresse, welche von den Schaltungsknoten verwendet wird, um das jeweilige Nachrichtenpaket an die geeignete Zielvorrichtung zu leiten. Adressen im Internet haben die Form von "n"-Bit Zahlen (wobei "n" beim gegenwärtigen Standard 32 oder 128 sein kann). Um insbesondere einen Bediener einer Vorrichtung 12(m) von der Notwendigkeit zu befreien, sich spezifische Zahlenkolonnen bzw. Zahlen-Internetadressen zu merken und diese der Vorrichtung 12(m) einzugeben, um die Erzeugung eines Nachrichtenpaketes zur Übertragung über das Internet einzuleiten, stellt das Internet 40 einen zweiten Adressierungsmechanismus zur Verfügung, welcher einfacher durch menschliche Bediener der jeweiligen Vorrichtungen handhabbar ist. Bei diesem Adressierungsmechanismus werden Internet-Domains, wie etwa LANs, Internet-Service-Provider (ISPs) und ähnliche, welche in bzw. mit dem Internet verbunden sind, durch relativ einfache les- und merkbare Namen, sog. Klartextnamen, identifiziert. Dabei soll sich hier die Bezeichnung "Klartextname" auf jede Art von Namenstext beziehen, z. B. auch auf Abkürzungen, generische Bezeichnungen, Phantasiebegriffe, etc. Um das System der Klartext-Domainnamen einzusetzen, ist der ISP 11 mit einem Namen-Server 17 (der auch als ein DNS Server (Domain Name Server) bezeichnet werden kann) verbunden, welcher die Klartext-Domainnamen auflösen bzw. in eine gültige Internetadresse umwandeln kann, um die geeignete Internetadresse für das in dem jeweiligen Klartextnamen angegebene Ziel bereitzustellen. Im allgemeinen kann der Namen-Server ein Teil des ISP 11 oder damit direkt verbunden sein, wie es in Fig. 1 gezeigt ist, oder er kann eine bestimmte Vorrichtung sein, welche 55 durch den ISP über das Internet zugänglich ist. Jedenfalls wenn sich die Vorrichtung 12(m) bei dem ISP 11 während einer Kommunikationssitzung einloggt, wird der ISP 11, wie oben hingewiesen wurde, verschiedene Internet-Proto- 60 65

kollparameter (IP-Parameter) zuordnen, welche die Vorrichtung 12(m) während der Kommunikationssitzung verwendet, und welche in dem Internetparameterspeicher 25 gespeichert sind. Diese IP-Parameter enthalten Informationen, wie

- (a) eine Internetadresse für die Vorrichtung 12(m), welche die Vorrichtung 12(m) während der Kommunikationssitzung identifiziert; und
- (b) die Identifizierung eines Namen-Servers 17, welchen die Vorrichtung 12(m) während der Kommunikationssitzung verwendet.

Wenn die Vorrichtung 12(m) Nachrichtenpakete zur Übertragung erzeugt, fügt sie ihre Internetadresse (obiger Punkt (a)) als die Quellenadresse ein. Die Vorrichtung(en) 13, welche die jeweiligen Nachrichtenpakete empfängt/empfangen, kann/können die Quellenadresse aus den Nachrichtenpaketen, welche von der Vorrichtung 12(m) empfangen werden, in Nachrichtenpaketen verwenden, welche die Vorrichtung(en) 13 zur Übertragung an die Vorrichtung 12(m) erzeugt/erzeugen, so daß das Internet in der Lage ist, die durch die jeweilige Vorrichtung 13 erzeugten Nachrichtenpakete an die Vorrichtung 12(m) zu leiten. Falls die Vorrichtung 12(m) auf den Namen-Server 17 über das Internet 14 zugreift, hat die durch den ISP 11 bereitgestellte Identifizierung des Namen-Servers 17 (siehe oben unter (b)) die Form einer Zahlen-Internetadresse, welche es der Vorrichtung 12(m) ermöglicht, für den Namen-Server 17 Nachrichten zu erzeugen, welche eine Auflösung der Klartext-Internetadressen in Zahlen-Internetadressen anfordern. Der ISP 11 kann der Vorrichtung 12(m) auch andere IP-Parameter zuordnen, wenn diese sich beim ISP 11 einloggt, beispielsweise die Identifizierung einer Verbindung zu dem Internet 14, welche für Nachrichten zu verwenden ist, die durch die Vorrichtung 12(m) übertragen werden, insbesondere falls der ISP 11 Mehrfach-Gateways aufweist. In der Regel speichert die Vorrichtung 12(m) die Internetparameter im Internetparameterspeicher 25 für die Verwendung während der Kommunikationssitzung.

Wenn ein Bediener die Vorrichtung 12(m) veranlassen möchte, daß sie ein Nachrichtenpaket an eine Vorrichtung 13 überträgt, gibt der oder die Bediener(in) die Internetadresse der Vorrichtung 13 an die Vorrichtung 12(m) über die Bedienerschnittstelle 20 ein, sowie eine Information oder die Identifizierung der in der Vorrichtung 12(m) aufbewahrten Information, welche in der Nachricht übertragen werden sollen. Die Bedienerschnittstelle 20 aktiviert daraufhin den Paketgenerator 22 zur Freigabe der benötigten Pakete zur Übertragung durch den ISP 11 über das Internet 14. Falls

- (i) der Bediener die Zahlen-Internetadresse bereitgestellt hat, oder
- (ii) der Bediener die Klartext-Internetadresse bereitgestellt hat, aber der Paketgenerator 22 bereits die Zahlen-Internetadresse besitzt, welche der durch den Bediener eingegebenen Klartext-Internetadresse entspricht,

kann der Paketgenerator 22 unmittelbar nach Aktivierung durch die Bedienerschnittstelle 20 die Pakete erzeugen und diese an die Netzwerkschnittstelle 21 zur Übertragung an den ISP 11 liefern.

Falls aber der Bediener die Klartext-Internetadresse der Vorrichtung 13, an welche die Pakete zu übertragen sind, eingegeben hat, und falls der Paketgenerator 22 die entsprechende Zahlen-Internetadresse davon nicht bereits besitzt,

ermöglicht es der Paketgenerator 22, daß die Netzwerkadresse von dem Namen-Server 17, der in dem IP-Parameterspeicher 25 identifiziert ist, erhalten wird.

Bei diesem Vorgang wird der Paketgenerator 22 anfänglich den Namen-Server 17 kontaktieren, um zu versuchen, die geeignete Zahlen-Internetadresse von dem Namen-Server 17 zu erhalten. Bei diesem Vorgang wird die Vorrichtung 12(m) geeignete Nachrichtenpakete zur Übertragung an den Namen-Server 17 unter Verwendung der Zahlen-Internetadresse des Namen-Servers 17 erzeugen, welche durch den ISP 11 bereitgestellt wird, wenn sich die Vorrichtung 12(m) zu Beginn der Kommunikationssitzung einloggt. Jedenfalls wenn der Namen-Server 17 die Zahlen-Internetadresse für den Klartextnamen besitzt oder erhalten kann, wird der Namen-Server 17 die Zahlen-Internetadresse an die Vorrichtung 12(m) übermitteln. Die Zahlen-Internetadresse wird durch den Paketgenerator 22 über die Netzwerkschnittstelle 21 und den Paketempfänger und -prozessor 23 empfangen. Nachdem der Paketgenerator 22 die Zahlen-Internetadresse empfangen hat, kann er die notwendigen Nachrichtenpakete zur Übertragung an die Vorrichtung 13 durch die Netzwerkschnittstelle 21 und den ISP 11 erzeugen.

Wie oben ausgeführt wurde, ist in Fig. 1 eine der Vorrichtungen 13, welche an das Internet 14 angeschlossen sind, ein virtuelles privates Netzwerk 15, wobei das virtuelle private Netzwerk 15 eine Firewall bzw. ein Firewall-System 30, mehrere als Server 31(s) gekennzeichnete Vorrichtungen und einen Namen-Server 32 aufweist, die durch eine Übertragungsverbindung 33 miteinander verbunden sind. Die Server 31(s), die Firewall 30 und der Namen-Server 32 können als z. B. in einem LAN oder WAN verbundene Vorrichtungen untereinander Information in Form von Nachrichtenpaketen austauschen. Da die Firewall 30 mit dem Internet 14 verbunden ist und darüber Nachrichtenpakete empfangen kann, hat sie auch eine Internetadresse. Zusätzlich haben wenigstens die Server 31(s), welche über das Internet zugänglich sind, auch jeweilige Internetadressen. Dabei dient der Namen-Server 32 der Umwandlung von Klartext-Internetadressen für die Server 31(s) innerhalb des virtuellen privaten Netzwerkes 15 in die jeweiligen Zahlen-Internetadressen.

Im allgemeinen wird das virtuelle private Netzwerke 15 von einem Unternehmen, einem Regierungsamt, einer Organisation oder ähnlichem gehalten, welche möchten, daß die Server 31(s) Zugriff auf andere Vorrichtungen außerhalb des virtuellen privaten Netzwerkes 15 haben und an diese Information über das Internet 14 übertragen können, aber welche ebenfalls möchten, daß der Zugriff an die Server 31(s) durch Vorrichtungen 12(m) und andere externe Vorrichtungen über das Internet 14 in einer kontrollierten Weise begrenzt ist. Die Firewall 30 dient dazu, den Zugriff durch Vorrichtungen außerhalb des virtuellen privaten Netzwerkes 15 auf Server 31(s) innerhalb des virtuellen privaten Netzwerkes 15 zu kontrollieren. Bei diesem Vorgang stellt die Firewall 30 auch die Verbindung zum Internet 14 her und empfängt Nachrichtenpakete darüber zur Übertragung an einen Server 31(s). Falls das Nachrichtenpaket angibt, daß die Quelle des Nachrichtenpaketes einen Zugriff auf einen bestimmten Server 31(s) anfordert, und falls die Quelle für den Zugriff an den Server 31(s) autorisiert ist, sendet die Firewall 30 das Nachrichtenpaket über die Übertragungsverbindung 33 an den Server 31(s). Falls andererseits die Quelle nicht autorisiert ist, auf den Server 31(s) zuzugreifen, wird die Firewall 30 das Nachrichtenpaket nicht an den Server 31(s) übersenden, und kann anstelle ein Antwortnachrichtenpaket an die Quellenvorrichtung übermitteln, welches angibt, daß die Quelle nicht für den Zugriff an den Server 31(s) autorisiert ist. Die Firewall kann ähnlich aufgebaut sein wie die ande-

ren Vorrichtungen 31(s) in dem virtuellen privaten Netzwerk 15, wobei zusätzlich eine oder mehrere Verbindungen mit dem Internet vorhanden sind, welche allgemein durch das Bezugszeichen 43 gekennzeichnet sind.

Kommunikationen zwischen Vorrichtungen außerhalb des virtuellen privaten Netzwerkes 15, z. B. der Vorrichtung 12(m), und einer Vorrichtung, z. B. einem Server 31(s), innerhalb des virtuellen privaten Netzwerkes 15 kann über einen Sicherheitstunnel zwischen der Firewall 30 und der externen Vorrichtung, wie es oben beschrieben ist, erreicht werden, damit die ausgetauschten Information geheim bleiben, während diese über das Internet 14 und durch den ISP 11 übertragen werden. Ein Sicherheitstunnel zwischen der Vorrichtung 12(m) und dem virtuellen privaten Netzwerk 15 ist in Fig. 1 durch logische Verbindungen dargestellt, welche durch die Bezugszeichen 40, 42 und 44 gekennzeichnet sind; es versteht sich, daß die logischen Verbindung 42 eine der logischen Verbindungen 41 zwischen dem ISP 11 und dem Internet 14 und die logische Verbindung 44 eine der logischen Verbindungen 43 zwischen dem Internet 14 und der Firewall 30 umfaßt.

Der Aufbau eines Sicherheitstunnels kann durch eine Vorrichtung 12(m), die extern zu dem virtuellen privaten Netzwerk 15 ist, ausgelöst werden. Bei diesem Vorgang erzeugt die Vorrichtung 12(m) in Reaktion auf eine Aufforderung durch deren Bediener ein Nachrichtenpaket zur Übertragung durch den ISP 11 und das Internet 14 an die Firewall 30, welches den Aufbau eines Sicherheitstunnels zwischen der Vorrichtung 12(m) und der Firewall 30 anfordert. Das Nachrichtenpaket kann an eine bestimmte Zahlen-Internetadresse gerichtet sein, welche der Firewall 30 zugeordnet ist und welche für Sicherheitstunnelaufbuanfragen reserviert ist, und welche ferner der Vorrichtung 12(m) bekannt ist und durch den Namen-Server 17 bereitgestellt wird. Falls die Vorrichtung 12(m) autorisiert ist, auf einen Server 31(s) in dem virtuellen privaten Netzwerk 15 zuzugreifen, nehmen die Vorrichtung 12(m) als Client und die Firewall 30 einen Dialog auf, welcher den Austausch von einem oder mehreren Nachrichtenpaketen über das Internet 14 umfaßt. Während des Dialogs kann die Firewall 30 der Vorrichtung 12(m) die Identifizierung eines Verschlüsselungsalgorithmus und einen zugehörigen Verschlüsselungsschlüssel bereitstellen, welche die Vorrichtung 12(m) beim Entschlüsseln der verschlüsselten Abschnitte der Nachrichtenpakete zu verwenden hat, welche das virtuelle private Netzwerk an die Vorrichtung 12(m) überträgt. Zusätzlich dazu kann die Firewall 30 der Vorrichtung 12(m) auch die Identifizierung eines Verschlüsselungsalgorithmus und einen zugehörigen Verschlüsselungsschlüssel bereitstellen, welche die Vorrichtung 12(m) beim Verschlüsseln der Abschnitte der Nachrichtenpakete zu verwenden hat, welche die Vorrichtung 12(m) an das virtuelle private Netzwerk 15 überträgt und welche verschlüsselt werden sollen. Alternativ dazu kann die Vorrichtung 12(m) die Identifizierung des Verschlüsselungsalgorithmus und des Verschlüsselungsschlüssels, welche die Vorrichtung 12(m) verwenden wird, an die Firewall 30 während des Dialogs liefern. Die Vorrichtung 12(m) kann in ihrem IP-Parameterspeicher 25 Informationen betreffend den Sicherheitstunnel speichern, einschließlich der Information in Verbindung mit der Identifizierung der Firewall 30 und der Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und dazugehöriger Schlüssel für Nachrichtenpakete, welche durch den Sicherheitstunnel übertragen werden.

Sodann können die Vorrichtung 12(m) und die Firewall 30 Nachrichtenpakete über den Sicherheitstunnel übertragen. Beim Erzeugen von Nachrichtenpaketen zur Übertragung über den Sicherheitstunnel verwendet die Vorrichtung

12(m) den Sicherheits-Paketprozessor 26, um die Abschnitte der Nachrichtenpakete zu verschlüsseln, welche vor der Übertragung durch die Netzwerkschnittstelle 21 an den ISP 11 zur Übertragung über das Internet 14 an die Firewall

- 5 30 verschlüsselt werden sollen, und um die verschlüsselten Abschnitte der Nachrichtenpakete zu entschlüsseln, welche durch die Vorrichtung 12(m) empfangen werden und welche verschlüsselt sind. Insbesondere nachdem der Paketgenerator 22 ein Nachrichtenpaket zur Übertragung an die Firewall
- 10 30 über den Sicherheitstunnel erzeugt hat, liefert er das Nachrichtenpaket an den Sicherheits-Paketprozessor 26. Der Sicherheits-Paketprozessor 26 verschlüsselt daraufhin die Abschnitte des Nachrichtenpakets, welche verschlüsselt werden sollen, unter Verwendung des Verschlüsselungsalgorithmus und des Verschlüsselungsschlüssels. Nachdem die Firewall 30 ein Nachrichtenpaket von der Vorrichtung 12(m) über den Sicherheitstunnel empfangen hat, wird sie dieses entschlüsseln und, falls der beabsichtigte Empfänger des Nachrichtenpakets eine andere Vorrichtung, z. B. ein
- 15 Server 31(s), in dem virtuellen privaten Netzwerk 15 ist, wird die Firewall 30 das Nachrichtenpaket an diese andere Vorrichtung über die Übertragungsverbindung 33 übertragen.

Wenn ein Nachrichtenpaket von einer Vorrichtung, z. B. einem Server 31(s), in dem virtuellen privaten Netzwerk 15 an die Vorrichtung 12(m) über den Sicherheitstunnel übertragen werden soll, empfängt die Firewall 30 ein solches Nachrichtenpaket über die Übertragungsverbindung 33 und verschlüsselt das Nachrichtenpaket zur Übertragung über das Internet 14 an den ISP 11. Der ISP 11 sendet daraufhin das Nachrichtenpaket an die Vorrichtung 12(m), insbesondere an deren Netzwerkschnittstelle 21. Die Netzwerkschnittstelle 21 liefert das Nachrichtenpaket an den Sicherheits-Paketprozessor 26, welcher die verschlüsselten Abschnitte des Nachrichtenpakets unter Verwendung des Entschlüsselungsalgorithmus und -schlüssels entschlüsselt.

Ein Problem tritt auf im Zusammenhang mit Zugriffen durch eine Vorrichtung, z. B. einer Vorrichtung 12(m), welche extern zum virtuellen privaten Netzwerk 15 ist, und einer Vorrichtung, z. B. einem Server 31(s), welche extern zu der Firewall ist, nämlich dann, wenn dem Namen-Server 17 keine Zahlen-Internetadressen für die Server 31(s) und andere Vorrichtungen bereitgestellt sind, die sich innerhalb des virtuellen privaten Netzwerkes 15 befinden – mit Ausnahme der Zahlen-Internetadressen, welche der Firewall 30 zugeordnet sind. Folglich wird die Vorrichtung 12(m) nach Eingabe der Klartext-Internetadresse durch den Bediener nicht in der Lage sein, die Zahlen-Internetadresse des Servers 31(s) zu erhalten, wenn er auf den Namen-Server 17 zugreift.

Wenn die Vorrichtung 12(m) und die Firewall 30 zusammenarbeiten, um einen dazwischenliegenden Sicherheitstunnel aufzubauen, liefert die Firewall 30 zur Behebung des obigen Problems an die Vorrichtung 12(m) zusätzlich zu möglichen Identifikationen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüsseln, welche im Zusammenhang mit der Übertragung der Nachrichtenpakete über den Sicherheitstunnel zu verwenden sind, an die Vorrichtung 12(m) auch die Identifizierung eines Namen-Servers, z. B. eines Namen-Servers 32, innerhalb des virtuellen privaten Netzwerkes 15, auf welchen die Vorrichtung 12(m) zugreifen kann, um die geeigneten Zahlen-Internetadressen für die Klartext-Internetadressen zu erhalten, welche durch den Bediener einer Vorrichtung 12(m) eingegeben werden. Die Identifizierung des Namen-Servers 32 wird ebenfalls in dem IP-Parameterspeicher 25 gespeichert, zusammen mit der Identifizierung des Namen-Servers 17, welche durch den ISP 11 bereitgestellt wurde, sobald die Vorrichtung 12(m)

beim ISP 11 zu Beginn einer Kommunikationssitzung eingeloggt wurde. Wenn daher die Vorrichtung 12(m) ein Nachrichtenpaket an eine Vorrichtung, z. B. einen Server 31(s), in dem virtuellen privaten Netzwerk 15 unter Verwendung einer Klartext-Internetadresse übertragen möchte, welche z. B. durch einen Bediener bereitgestellt bzw. eingegeben wurde, greift die Vorrichtung 12(m) zu Beginn auf den Namen-Server 17 zu, wie es oben beschrieben wurde, um zu versuchen, die zu der Klartext-Internetadresse zugehörige Zahlen-Internetadresse zu erhalten. Da der Namen-Server 17 außerhalb des virtuellen privaten Netzwerkes 15 ist und die durch die Vorrichtung 12(m) angeforderten Information nicht besitzt, sendet er ein entsprechend lautendes Antwortnachrichtenpaket. Die Vorrichtung 12(m) wird sodann ein Anfragenachrichtenpaket zur Übertragung an den Namen-Server 32 durch die Firewall 30 und über den Sicherheitstunnel erzeugen. Falls der Namen-Server 32 eine Zahlen-Internetadresse besitzt, welche zu der Klartext-Internetadresse in dem Anfragenachrichtenpaket gehört, welches durch die Vorrichtung 12(m) geliefert wird, stellt er die Zahlen-Internetadresse in einer Weise bereit, welche im allgemeinen derjenigen ähnlich ist, welche oben im Zusammenhang mit dem Namen-Server 17 beschrieben wurde mit der Ausnahme, daß die Zahlen-Internetadresse durch den Namen-Server 32 in einem an die Firewall 30 gerichteten Nachrichtenpaket geliefert wird, und die Firewall 30 sodann das Nachrichtenpaket über den Sicherheitstunnel an die Vorrichtung 12(m) übermittelt. Es versteht sich, daß sich in dem Nachrichtenpaket, welches durch die Firewall 30 übertragen wird, die Zahlen-Internetadresse in dem Nachrichtenpaket im Datenabschnitt des Nachrichtenpakets befindet, welches über den Sicherheitstunnel übertragen wird und entsprechend verschlüsselt sein wird. Das Nachrichtenpaket wird durch die Vorrichtung 12(m) in einer ähnlichen Weise verarbeitet, wie sie oben im Zusammenhang mit anderen Nachrichtenpaketen beschrieben wurde, welche durch die Vorrichtung 12(m) über den Sicherheitstunnel empfangen werden. Das heißt, daß das Nachrichtenpaket durch den Sicherheits-Paketprozessor 26 vor dem Übermitteln an den Paketempfänger und -prozessor 23 zur Verarbeitung entschlüsselt wird. Die Zahlen-Internetadresse für den Server 31(s) kann in einem Cache in einer Zugriffskontrolliste (ACL) in dem IP-Parameterspeicher 25 gespeichert werden, zusammen mit der Zuordnungsinformation bezüglich der zugehörigen Klartext-Internetadresse, einer Angabe, daß der Server 31(s), der dieser Klartext-Internetadresse zugeordnet ist, über die Firewall 30 des virtuellen privaten Netzwerkes 15 zugänglich ist, und die Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel, welche für eine Verschlüsselung und Entschlüsselung der geeigneten Abschnitte der Nachrichtenpakete zu verwenden sind, welche an den Server 31(s) übertragen und von diesem erhalten werden.

Es versteht sich, daß in Reaktion auf ein Nachrichtenpaket von der Vorrichtung 12(m), welches beim Namen-Server 32 die Bereitstellung einer Zahlen-Internetadresse für eine durch die Vorrichtung 12(m) angegebene Klartext-Internetadresse anfordert, falls der Namen-Server 32 keine Zuordnungsinformation zwischen der Klartext-Internetadresse und einer Zahlen-Internetadresse besitzt, der Namen-Server 32 ein Antwortnachrichtenpaket, das entsprechend lautet, übertragen kann. Falls die Vorrichtung 12(m) eine Identifizierung von anderen Namen-Servern besitzt, welche z. B. mit anderen virtuellen privaten Netzwerken (nicht gezeigt) verbunden sein können und zu welchen die Vorrichtung 12(m) Zugriff hat, dann kann die Vorrichtung 12(m) versuchen, auf die anderen Namen-Server in einer ähnlichen Weise, wie es oben beschrieben ist, zuzugreifen. Falls die

Vorrichtung 12(m) nicht in der Lage ist, eine Zahlen-Internetadresse, welche der Klartext-Internetadresse zugeordnet ist, von irgendeinem der Namen-Server zu erhalten, zu welchem sie Zugriff hat und welche im allgemeinen im IP-Parameterspeicher 25 der Vorrichtung 12(m) identifiziert sind, wird sie allgemein nicht in der Lage sein, auf eine Vorrichtung mit der vorgegebenen Klartext-Internetadresse zuzugreifen und wird den Bediener oder ein Programm, welche den Zugriff angefordert haben, dementsprechend unterrichten.

Mit diesem Hintergrund werden nun Operationen, welche durch die Vorrichtung 12(m) und das virtuelle private Netzwerk 15 in Verbindung mit der vorliegenden Erfindung durchgeführt werden, im Detail beschrieben. Im allgemeinen laufen die Operationen in zwei Phasen ab. In einer ersten Phase arbeiten die Vorrichtung 12(m) und das virtuelle private Netzwerk 15 zusammen, um einen Sicherheitstunnel durch das Internet 14 aufzubauen. In dieser ersten Phase liefert das virtuelle private Netzwerk 15, insbesondere die Firewall 30, die Identifizierung eines Namen-Servers 32, und es kann auch die den Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel betreffende Information bereitstellen, wie es oben beschrieben wurde. In der zweiten Phase, nachdem der Sicherheitstunnel eingerichtet wurde, kann die Vorrichtung 12(m) die während der ersten Phase gelieferten Information im Zusammenhang mit der Erzeugung und Übertragung von Nachrichtenpaketen an einen oder mehrere Server 31(s) in dem virtuellen privaten Netzwerk 15 und bei dem notwendigen Umwandlungsvorgang der Klartext-Internetadressen zu Zahlen-Internetadressen aus dem Namen-Server 32, welcher durch die Firewall 30 während der ersten Phase identifiziert wurde, verwenden.

Folglich erzeugt die Vorrichtung 12(m) in der ersten (Sicherheitstunnelaufbau)phase zu Beginn ein Nachrichtenpaket zur Übertragung an die Firewall 30, welches einen Aufbau eines Sicherheitstunnels anfordert. Das Nachrichtenpaket enthält eine Zahlen-Internetadresse für die Firewall, (welche durch den Bediener der Vorrichtung oder ein Programm bereitgestellt werden kann, welches durch die Vorrichtung 12(m) verarbeitet wird, oder durch den Namen-Server 17 bereitgestellt werden kann, nachdem eine Klartext-Internetadresse durch den Bediener oder ein Programm bereitgestellt wurde), und welche insbesondere dazu dient, die Firewall 30 zu veranlassen, mit der Vorrichtung 12(m) einen Sicherheitstunnel aufzubauen. Falls die Firewall 30 die Anfrage bezüglich des Sicherheitstunnelaufbaus akzeptiert und falls die Firewall 30 die Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel bereitstellt, so wie es oben angegeben wurde, erzeugt die Firewall 30 ein Antwortnachrichtenpaket zur Übertragung an die Vorrichtung 12(m), welches die Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel identifiziert. Wie oben beschrieben, wird dieses Antwortnachrichtenpaket nicht verschlüsselt. Wenn die Vorrichtung 12(m) die Antwort empfängt, werden die Identifizierungen der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel in dem IP-Parameterspeicher 25 gespeichert.

Zu einem späteren Zeitpunkt in der ersten Phase erzeugt die Firewall 30 auch ein Nachrichtenpaket zur Übertragung an die Vorrichtung 12(m), welches die Zahlen-Internetadresse des Namen-Servers 32 enthält. Bei diesem Nachrichtenpaket wird der Abschnitt des Nachrichtenpakets, welcher die Zahlen-Internetadresse des Namen-Servers 32 enthält, unter Verwendung eines Verschlüsselungsalgoritmus und Verschlüsselungsschlüssels verschlüsselt, und dies kann unter Verwendung des Entschlüsselungsalgoritmus und -schlüssels, die durch das zuvor beschriebene Antwortnachrichtenpaket geliefert wurden, wieder entschlüsselt

werden. Diese Nachricht hat im allgemeinen die folgende Struktur:

"<IIA(FW),IIA(DEV12(m))><SEC\_TUN>  
<ENCR<<IIA(FW),IIA(DEV\_12(m))><(DNS\_ADRS:IIA-  
NS\_2>>>"

wobei

- (i) "IIA(FW)" die Quellenadresse darstellt, d. h. eine Zahlen-Internetadresse der Firewall 30,
- (ii) "IIA(DEV\_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung 12(m),
- (iii) "DNS\_ADRS:IIA(NS)" angibt, daß "IIA(NS\_32)" die Zahlen-Internetadresse des Namen-Servers 32 darstellt, für dessen Benutzung die Vorrichtung 12(m) autorisiert ist, und
- (iv) "ENCR<...>" bedeutet, daß die Information, zwischen den Klammern "<" und ">" verschlüsselt ist.

Der Anfangsabschnitt der Nachricht "<IIA(FW),IIA(DEV\_12(m))>" bildet wenigstens einen Teil des Kopfabschnitts der Nachricht, und "<ENCR<<IIA(FW),IIA(DEV\_12(m))><IIA(NS)>>>" stellt wenigstens einen Teil des Datenabschnitts der Nachricht dar. "<SEC\_TUN>" stellt einen Hinweis in dem Kopfabschnitt dar, welcher angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, wodurch auch angezeigt wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält.

Nachdem die Vorrichtung 12(m) die Nachricht von der Firewall 30 empfängt, wie es oben beschrieben wurde, und weil das Nachrichtenpaket den <SEC\_TUN> Hinweis enthält, überträgt deren Netzwerkschnittstelle 21 den verschlüsselten Abschnitt "<ENCR<<IIA(FW),IIA(DEV\_12(m))><DNS\_ADRS:IIA-  
NS\_32>>>" an den Sicherheits-Paketprozessor 26 zur Verarbeitung. Der Sicherheits-Paketprozessor 26 entschlüsselt den verschlüsselten Abschnitt, bestimmt weiter, daß der Abschnitt "IIA(NS\_32)" die Zahlen-Internetadresse des Namen-Servers darstellt, insbesondere des Namen-Servers 32, für dessen Benutzung die Vorrichtung 12(m) autorisiert ist, und speichert diese Adresse in dem IP-Parameterspeicher 25 zusammen mit einer Angabe, daß die dorthin gerichteten Nachrichtenpakete zu der Firewall 30 zu übertragen sind, und daß die Daten in den Nachrichtenpaketen unter Verwendung des Verschlüsselungsalgorithmus und -schlüssels, die davor durch die Firewall 30 übermittelt wurden, zu verschlüsseln sind. Es versteht sich, daß aufgrund der Tatsache, daß die Zahlen-Internetadresse des Namen-Servers 32 von der Firewall an die Vorrichtung 12(m) in verschlüsselter Form übertragen wird, diese vertraulich bleibt, selbst wenn das Paket durch einen Dritten abgefangen wird.

In Abhängigkeit des speziellen Protokolls, welches für den Aufbau des Sicherheitstunnels verwendet wird, können die Firewall 30 und die Vorrichtung 12(m) auch Nachrichtenpakete austauschen, welche andere Information enthalten als die oben beschriebenen.

Wie oben erwähnt wurde, kann die Vorrichtung 12(m) in der zweiten Phase nach der Einrichtung des Sicherheitstunnels die Information, welche während der ersten Phase bereitgestellt wurde, im Zusammenhang mit dem Erzeugen und Übertragen von Nachrichtenpaketen zu einem oder mehreren der Server 31(s) in dem virtuellen privaten Netzwerk 15 nutzen. Falls bei diesen Operationen der Bediener einer Vorrichtung 12(m) oder ein Programm, welches durch eine Vorrichtung 12(m) verarbeitet wird, möchte, daß die Vorrichtung 12(m) ein Nachrichtenpaket an einen Server

31(s) in dem virtuellen privaten Netzwerk 15 überträgt, und falls der Bediener durch die Bedienerchnittstelle 20 oder das Programm eine Klartext-Internetadresse bereitstellt, wird zunächst die Vorrichtung 12(m), insbesondere der Paketgenerator 22, bestimmen, ob der IP-Parameterspeicher 25 dort in einem Cache eine Zahlen-Internetadresse gespeichert hat, welche zu der Klartext-Internetadresse gehört.

Falls dies nicht der Fall ist, erzeugt der Paketgenerator 22 ein Anfragenachrichtenpaket zur Übertragung an den Namen-Server 17, um von diesem die zu der Klartext-Internetadresse gehörige Zahlen-Internetadresse anzufordern. Falls der Namen-Server 17 eine zu der Klartext-Internetadresse gehörige Zahlen-Internetadresse besitzt, wird dieser die Zahlen-Internetadresse an die Vorrichtung 12(m) liefern. Es versteht sich, daß dies nur erfolgen kann, wenn die Klartext-Internetadresse im Anfragenachrichtenpaket sowohl einer Vorrichtung 13 außerhalb des virtuellen privaten Netzwerkes 15 als auch einem Server 32(s) in dem virtuellen privaten Netzwerk 15 zugeordnet wurde. Danach kann die Vorrichtung 12(m) die Zahlen-Internetadresse verwenden, um Nachrichtenpakete zur Übertragung über das Internet zu erzeugen, wie es oben beschrieben wurde.

Falls andererseits angenommen wird, daß der Namen-Server 17 keine der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse besitzt, wird der Namen-Server 17 ein entsprechend lautendes Antwortnachrichtenpaket an die Vorrichtung 12(m) übermitteln. Sodann erzeugt der Paketgenerator 22 der Vorrichtung 12(m) ein Anfragenachrichtenpaket zur Übertragung an den nächsten Namen-Server, der in ihrem IP-Parameterspeicher 25 identifiziert ist, um von diesem Namen-Server die der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse anzufordern. Falls dieser nächste Namen-Server der Namen-Server 32 ist, liefert der Paketgenerator 22 das Nachrichtenpaket an den Sicherheits-Paketprozessor 26 zur weiteren Verarbeitung. Der Sicherheits-Paketprozessor 26 erzeugt daraufhin ein Anfragenachrichtenpaket zur Übertragung über den Sicherheitstunnel an die Firewall 30. Diese Nachricht hat im allgemeinen folgende Struktur:

"<IIA(DEV\_12(m)),IIA(FW)><SEC\_TUN>  
<ENCR<<IIA(DEV\_12(m)),IIA(NS\_32)><IIA\_REQ>>>"

wobei

- (i) "IIA(DEV\_12(m))" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung 12(m),
- (ii) "IIA(FW)" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Firewall 30,
- (iii) "IIA(NS\_32)" die Adresse des Namen-Servers 32 darstellt,
- (iv) "<<IIA(DEV\_12(m)),IIA(NS\_32)><IIA\_REQ>>>" das Anfragenachrichtenpaket darstellt, welches durch den Paketgenerator 22 erzeugt wird, wobei "<IIA(DEV\_12(m)),IIA(NS\_32)>" den Kopfabschnitt des Anfragenachrichtenpaketes und "<IIA\_REQ>" den Datenabschnitt des Anfragenachrichtenpaketes darstellt,
- (v) "ENCR<...>" angibt, daß die Information zwischen den Klammern "<" und ">" verschlüsselt ist, und
- (vi) "<SEC\_TUN>" einen Hinweis in dem Kopfabschnitt des Nachrichtenpakets darstellt, welches durch den Sicherheitspaketgenerator 26 erzeugt wird und angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, wobei hierdurch angegeben wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält.

Wenn die Firewall 30 das durch den Sicherheitspaketgenerator 26 erzeugte Anfragenachrichtenpaket empfängt, wird diese den verschlüsselten Abschnitt des Nachrichtenpakets entschlüsseln, um "«IIA(DEV\_12(m)),IIA(NS\_32)><IIA\_REQ>>" zu erhalten. Dies stellt das Anfragenachrichtenpaket dar, welches durch den Paketgenerator 22 erzeugt wird. Nachdem das Anfragenachrichtenpaket erhalten wurde, überträgt die Firewall 30 dieses über die Übertragungsverbindung 33 an den Namen-Server 32. In Abhängigkeit von dem Protokoll zur Übertragung von Nachrichtenpaketen über die Übertragungsverbindung 33 kann es bei diesem Prozeß für die Firewall 30 notwendig sein, das Anfragenachrichtenpaket zu modifizieren, damit es dem Protokoll der Übertragungsverbindung 33 entspricht.

Nachdem der Namen-Server 32 das Anfragenachrichtenpaket erhalten hat, wird dieser das Anfragenachrichtenpaket verarbeiten, um zu bestimmen, ob er eine der Klartext-Internetadresse, welche in dem Anfragenachrichtenpaket gesendet wird, zugeordnete Zahlen-Internetadresse besitzt. Falls der Namen-Server feststellt, daß er eine solche Zahlen-Internetadresse aufweist, wird dieser ein Antwortnachrichtenpaket zur Übertragung an die Firewall erzeugen, welches die Zahlen-Internetadresse enthält. Im allgemeinen hat das Antwortnachrichtenpaket die folgende Struktur:

"«IIA(NS\_32),IIA(DEV\_12(m)><IIA\_RESP>>"

wobei

- (i) "IIA(NS\_32)" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse des Namen-Servers 32,
- (ii) "IIA(DEV\_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung 12(m), und
- (iii) "IIA\_RESP" die Zahlen-Internetadresse darstellt, welche der Klartext-Internetadresse zugeordnet ist.

Nachdem die Firewall 30 das Antwortnachrichtenpaket empfangen hat, und weil die Kommunikation mit der Vorrichtung 12(m) über den dazwischenliegenden Sicherheitstunnel stattfindet, verschlüsselt die Firewall 30 das von dem Namen-Server 32 empfangene Antwortnachrichtenpaket und erzeugt ein Nachrichtenpaket zur Übertragung an die Vorrichtung 12(m), welches das verschlüsselte Antwortnachrichtenpaket enthält. Im allgemeinen hat das durch die Firewall 30 erzeugte Nachrichtenpaket die folgende Struktur:

"«IIA(FW),IIA(DEV12(m)><SEC\_TUN>>  
<ENCR<IIA(NS\_32),IIA(DEV\_12(m)><IIA\_RESP>>>"

wobei

- (i) "IIA(FW)" die Quellenadresse darstellt, d. h. die Zahlen-Internetadresse der Firewall 30,
- (ii) "IIA(DEV\_12(m))" die Zieladresse darstellt, d. h. die Zahlen-Internetadresse der Vorrichtung 12(m),
- (iii) "SEC\_TUN" einen Hinweis in dem Kopfabschnitt des Nachrichtenpakets darstellt, welches durch den Sicherheitspaketgenerator 26 erzeugt wird, und angibt, daß die Nachricht über den Sicherheitstunnel übertragen wird, und wobei auch angegeben wird, daß der Datenabschnitt der Nachricht verschlüsselte Information enthält,
- (iv) "ENCR<...>" angibt, daß die Information zwischen den Klammern "<" und ">" (was dem von dem Namen-Server 32 empfangenen Antwortnachrichten-

paket entspricht) verschlüsselt ist.

Zusätzlich kann es je nach dem Protokoll zur Übertragung von Nachrichtenpaketen über die Übertragungsverbindung 33 für die Firewall 30 notwendig sein, das Nachrichtenpaket zu bearbeiten und/oder zu modifizieren, damit dieses dem Protokoll des Internets 14 entspricht.

Wenn die Vorrichtung 12(m) das Nachrichtenpaket von der Firewall 30 empfängt, wird das Nachrichtenpaket an den Sicherheits-Paketprozessor 26 geliefert. Der Sicherheitspaketprozessor 26 entschlüsselt daraufhin den verschlüsselten Abschnitt des Nachrichtenpakets, um die der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse zu erhalten und lädt diese Information in den IP-Parameterspeicher 25. Danach kann die Vorrichtung diese Zahlen-Internetadresse beim Erzeugen von Nachrichtenpaketen zur Übertragung an den Server 31(s) verwenden, welcher zu der Klartext-Internetadresse gehört.

Es versteht sich, daß, falls der Namen-Server 32 keine Zahlen-Internetadresse besitzt, welche der durch die Vorrichtung 12(m) in dem Anfragenachrichtenpaket gelieferte Klartext-Internetadresse zugeordnet ist, dies der Namen-Server 32 in dem durch ihn erzeugten Antwortnachrichtenpaket entsprechend anzeigen. Die Firewall 30 erzeugt dann in Reaktion auf das durch den Namen-Server 32 gelieferte Antwortnachrichtenpaket auch ein Nachrichtenpaket zur Übertragung an die Vorrichtung 12(m), welches einen verschlüsselten Abschnitt enthält, der das Antwortnachrichtenpaket umfaßt, das durch den Namen-Server 32 erzeugt wurde. Nachdem die Vorrichtung 12(m) das Nachrichtenpaket empfangen hat, wird der verschlüsselte Abschnitt durch den Sicherheitspaketprozessor 26 entschlüsselt, welcher daraufhin den Paketgenerator 22 darüber informiert, daß der Namen-Server 32 keine der Klartext-Internetadresse zugeordnete Zahlen-Internetadresse besitzt. Falls der IP-Parameterspeicher 25 die Identifizierung eines anderen Namen-Servers enthält, erzeugt sodann der Paketgenerator 22 der Vorrichtung 12(m) ein Anfragenachrichtenpaket zur Übertragung an den nächsten Namen-Server, der in deren IP-Parameterspeicher 25 identifiziert ist, um von diesem Namen-Server die Zahlen-Internetadresse anzufordern, welche der Klartext-Internetadresse zugeordnet ist. Falls andererseits der IP-Parameterspeicher 25 keine Identifizierung eines anderen Namen-Servers enthält, kann der Paketgenerator 22 die Bedienerschnittstelle 20 oder ein Programm darüber informieren, daß er nicht in der Lage ist, ein Nachrichtenpaket zur Übertragung an eine Vorrichtung zu erzeugen, welche der Klartext-Internetadresse zugeordnet ist, welche durch die Bedienerschnittstelle 20 oder ein Programm eingegeben bzw. bereitgestellt wurde.

Die Erfindung liefert eine Anzahl von Vorteilen. Insbesondere schafft die Erfindung ein System zum Vereinfachen der Kommunikation zwischen Vorrichtungen, welche mit einem öffentlichen Netzwerk verbunden sind, z. B. mit dem Internet 14, und Vorrichtungen, welche mit privaten Netzwerken verbunden sind, z. B. mit dem virtuellen privaten Netzwerk 15, indem die Umwandlung von Klartextadressen in Netzwerkadressen durch einen Namen-Server, der bevorzugt über einen Sicherheitstunnel mit den privaten Netzwerken verbunden ist, ermöglicht wird.

Es versteht sich, daß eine Vielzahl von Modifikationen an der im Zusammenhang mit Fig. 1 beschriebenen Anordnung durchgeführt werden können. Obwohl das Netzwerk 10 so beschrieben wurde, daß die Identifizierung der Verschlüsselungs- und Entschlüsselungsalgorithmen und -schlüssel durch die Vorrichtung 12(m) und die Firewall 30 während des Dialogs, währenddessen der Sicherheitstunnel eingerichtet wird, ausgetauscht wird, versteht es sich, daß bei

spielsweise Information durch die Vorrichtung 12(m) und die Firewall 30 getrennt von dem Aufbau eines solchen Sicherheitstunnels bereitgestellt werden können.

Obwohl die Erfindung im Zusammenhang mit dem Internet beschrieben wurde, versteht es sich ferner, daß die Erfindung in Verbindung mit jedem, insbesondere globalen, Netzwerk verwendet werden kann. Obwohl die Erfindung im Zusammenhang mit einem Netzwerk beschrieben wurde, welches ein System von Klartext-Netzwerkadressen bereitstellt, versteht es sich ferner, daß die Erfindung nicht darauf beschränkt ist sondern in Verbindung mit jedem Netzwerk verwendet werden kann, welches irgendeine Form einer – den systemeigenen Netzwerkadressen übergeordnete – Sekundär-Netzwerkadresseneinrichtung oder vergleichbare nicht-formelle Netzwerkadresseneinrichtung vorsieht. 15

Es versteht sich ferner, daß ein erfundungsgemäßes System als ganzes oder in Teilen aus speziell hierfür geeigneter Hardware oder einem allgemein geeigneten Computersystem oder jeder Kombination davon aufgebaut werden kann, wobei jeder Abschnitt davon durch ein geeignetes Programm gesteuert werden kann. Jedes Programm kann als ganzes oder in Teilen einen Teil des Systems umfassen oder auf dem System in einer konventionellen Weise gespeichert sein, oder es kann als ganzes oder in Teilen in das System über ein Netzwerk oder andere Mechanismen zur Übertragung von Information in einer konventionellen Weise bereitgestellt werden. Zusätzlich versteht es sich, daß das System betrieben und/oder auf andere Art und Weise mittels Information gesteuert werden kann, welche durch einen Bediener mittels Bedienereingabeelementen (nicht gezeigt) bereitgestellt wird, welche direkt an das System angeschlossen sein können oder welche die Information über ein Netzwerk oder andere Mechanismen zur Übertragung von Information in einer konventionellen Weise übertragen können. 20 25 30

Die vorstehende Beschreibung hat sich auf ein spezifisches Ausführungsbeispiel der Erfindung bezogen. Es versteht sich jedoch, daß verschiedene Variationen und Modifikationen der Erfindung gemacht werden können, bei welchen einige oder alle der Vorteile der Erfindung erreicht werden. Diese und andere Variationen und Modifikationen fallen in den Schutzbereich der vorliegenden Erfindung, der durch die nachfolgenden Ansprüche bestimmt ist. 35 40 45

#### Patentansprüche

1. System umfassend ein virtuelles privates Netzwerk (15) und eine externe Vorrichtung (12 (m)), welche über ein digitales Netzwerk (14) kommunizieren, wobei:  
das virtuelle private Netzwerk (15) eine Firewall (30), 50 wenigstens eine interne Vorrichtung (31(s)) und einen Namen-Server (32) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (31(s)) auch eine Sekundäradresse besitzt und der Namen-Server (32) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt,  
die Firewall (30) derart konfiguriert ist, daß sie der externen Vorrichtung (12(m)) in Reaktion auf deren Anfrage zum Aufbau einer Verbindung zur Firewall (30) 60 die Netzwerkadresse des Namen-Servers (32) liefert, und  
die externe Vorrichtung (12(m)) derart konfiguriert ist, daß sie in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (31(s)), welche die Sekundär- 65 Adresse der internen Vorrichtung (31(s)) enthält, eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (30) erzeugt, wel-

che eine Auflösung der der Sekundäradresse zugeordneten Netzwerkadresse anfordert, wobei die Firewall (30) derart konfiguriert ist, daß sie die Adressenauflösungsanfrage an den Namen-Server (32) übermittelt, der Namen-Server (32) derart konfiguriert ist, daß er die Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und die Firewall (30) daraufhin die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (12(m)) bereitstellt. 5

2. System nach Anspruch 1, bei welchem die externe Vorrichtung (12(m)) derart konfiguriert ist, daß sie die in der Netzwerkadressen-Antwortnachricht bereitgestellte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (31(s)) verwendet.
3. System nach Anspruch 1 oder 2, bei welchem die externe Vorrichtung (12(m)) derart konfiguriert ist, daß sie mit dem Netzwerk (14) durch einen Netzwerk-Service-Provider (11) verbunden wird.
4. System nach Anspruch 3, bei welchem die externe Vorrichtung (12(m)) derart konfiguriert ist, daß sie eine Kommunikationssitzung mit dem Netzwerk-Service-Provider (11) aufbaut, wobei der Netzwerk-Service-Provider (11) der externen Vorrichtung (12(m)) die Identifizierung eines weiteren Namen-Servers übermittelt, wobei der weitere Namen-Server derart konfiguriert ist, daß er eine Zuordnung zwischen einer Sekundäradresse und einer Netzwerkadresse für wenigstens eine Vorrichtung bereitstellt.
5. System nach einem der vorstehenden Ansprüche, bei welchem die externe Vorrichtung (12(m)) derart konfiguriert ist, daß sie eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (12(m)) identifiziert wurden, und die externe Vorrichtung (12(m)) die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (12(m)) eine Netzwerkadresse empfängt, wobei die externe Vorrichtung (12(m)) in jedem Abfragevorgang eine Netzwerkadressen-Anfragenachricht zur Übertragung über das Netzwerk (14) erzeugt, welche durch einen der Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-Antwortnachricht empfängt.
6. System nach einem der vorstehenden Ansprüche, bei welchem die Verbindung zwischen der externen Vorrichtung (12(m)) und der Firewall (30) ein Sicherheitstunnel ist, in welchem wenigstens ein der zwischen der externen Vorrichtung (12(m)) und der Firewall (30) übertragenen Nachrichten verschlüsselt ist.
7. Verfahren zum Betreiben eines Systems umfassend ein virtuelles privates Netzwerk (15) und eine externe Vorrichtung (12(m)), welche durch ein digitales Netzwerk (14) miteinander verbunden sind, wobei das virtuelle private Netzwerk (15) eine Firewall (30), wenigstens eine interne Vorrichtung (31(s)) und einen Namen-Server (32) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (31(s)) auch eine Sekundäradresse besitzt, und der Namen-Server (32) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt, wobei:
  - A. in Reaktion auf eine Anfrage der externen Vorrichtung (12(m)) zum Aufbau einer Verbindung zur Firewall (30) die Firewall (30) der externen Vorrichtung (12(m)) die Netzwerkadresse des

Namen-Servers (32) übermittelt; und

B. (i) in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (31(s)), welche die Sekundäradresse der internen Vorrichtung (31(s)) enthält, die externe Vorrichtung (12(m)) eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (30) erzeugt, welche eine Auflösung der Netzwerkadresse, welche der Sekundäradresse zugeordnet ist, anfordert,

(ii) die Firewall (30) die Adressenauflösungsanfrage an den Namen-Server (32) übermittelt, (iii) der Namen-Server (32) die der Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und

(iv) die Firewall (30) die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (12(m)) bereitstellt.

8. Verfahren nach Anspruch 7, bei welchem die externe Vorrichtung (12(m)) ferner die in der Netzwerkadressen-Antwortnachricht bereitgestellte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (31(s)) verwendet.

9. Verfahren nach Anspruch 7 oder 8, bei welchem die externe Vorrichtung (12(m)) mit dem Netzwerk (14) durch einen Netzwerk-Service-Provider (11) verbunden werden kann.

10. Verfahren nach Anspruch 9, bei welchem die externe Vorrichtung (12(m)) eine Kommunikationssitzung mit dem Netzwerk-Service-Provider (11) aufbaut, wobei der Netzwerk-Service-Provider (11) der externen Vorrichtung (12(m)) die Identifizierung eines weiteren Namen-Servers übermittelt, wobei der weitere Namen-Server eine Zuordnung zwischen einer Sekundäradresse und einer Netzwerkadresse für wenigstens eine Vorrichtung bereitstellt.

11. Verfahren nach einem der Ansprüche 7 bis 10, bei welchem die externe Vorrichtung (12(m)) eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (12(m)) identifiziert wurden, und die externe Vorrichtung (12(m)) die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (12(m)) eine Netzwerkadresse empfängt, wobei die externe Vorrichtung (12(m)) in jedem Abfragevorgang eine Netzwerkadressen-Anfragenachricht zur Übertragung über das Netzwerk (14) erzeugt, welche durch einen Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-Antwortnachricht empfängt.

12. Verfahren nach einem der Ansprüche 7 bis 11, bei welchem die Verbindung zwischen der externen Vorrichtung (12(m)) und der Firewall (30) ein Sicherheitstunnel ist, in welchem wenigstens ein Abschnitt der zwischen der externen Vorrichtung (12(m)) und der Firewall (30) übertragenen Nachrichten verschlüsselt ist.

13. Computerprogramm-Produkt zur gemeinsamen Verwendung mit einem virtuellen privaten Netzwerk (15) und einer externen Vorrichtung (12(m)), welche durch ein digitales Netzwerk (14) miteinander verbunden sind, wobei das virtuelle private Netzwerk eine Firewall (30), wenigstens eine interne Vorrichtung (31(s)) und einen Namen-Server (32) aufweist, welche jeweils eine Netzwerkadresse besitzen, wobei die interne Vorrichtung (31(s)) auch eine Sekundäradresse

besitzt, und der Namen-Server (32) derart konfiguriert ist, daß er eine Zuordnung zwischen der Sekundäradresse und der Netzwerkadresse bereitstellt, wobei das Computerprogrammprodukt ein maschinenlesbares Medium mit folgenden Codes aufweist:

A. ein Namen-Server-Identifizierungscodemodul, welches veranlaßt, daß die Firewall (30) der externen Vorrichtung (12(m)) in Reaktion auf deren Anfrage zum Aufbau einer Verbindung zur Firewall (30) die Netzwerkadresse des Namen-Servers (32) übermittelt,

B. ein Codemodul zur Erzeugung einer Netzwerkadressen-Anfragenachricht, welches veranlaßt, daß die externe Vorrichtung (12(m)) in Reaktion auf eine Anfrage zum Zugriff auf die interne Vorrichtung (31(s)), welche die Sekundäradresse der internen Vorrichtung (31(s)) enthält, eine Netzwerkadressen-Anfragenachricht zur Übertragung über die Verbindung an die Firewall (30) erzeugt, welche die Auflösung der Sekundäradresse zugeordneten Netzwerkadresse anfordert,

C. ein Modul zur Übermittlung einer Adressenauflösungsanfrage, welches veranlaßt, daß die Firewall (30) die Adressenauflösungsanfrage an den Namen-Server (32) übermittelt,

D. ein Namen-Server-Steuerungsmodul, welches veranlaßt, daß der Namen-Server (32) die der Sekundäradresse zugeordnete Netzwerkadresse bereitstellt, und

E. ein Modul zur Übermittlung einer Netzwerkadressen-Antwortnachricht, welches veranlaßt, daß die Firewall (30) die Netzwerkadresse in einer Netzwerkadressen-Antwortnachricht zur Übertragung über die Verbindung an die externe Vorrichtung (12(m)) bereitstellt.

14. Computerprogramm-Produkt nach Anspruch 13, welches ferner ein Netzwerkadressenverwendungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (12(m)) die in der Netzwerkadressen-Antwortnachricht übermittelte Netzwerkadresse beim Erzeugen von wenigstens einer Nachricht zur Übertragung an die interne Vorrichtung (31(s)) verwendet.

15. Computerprogramm-Produkt nach Anspruch 13 oder 14, welches ferner ein Netzwerk-Service-Provider-Steuerungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (12(m)) mit dem Netzwerk (14) durch einen Netzwerk-Service-Provider (11) verbunden wird.

16. Computerprogramm-Produkt nach Anspruch 15, bei welchem das Netzwerk-Service-Provider-Steuerungsmodul ein Kommunikationssitzungsaufbaumodul umfaßt, welches veranlaßt, daß die externe Vorrichtung (12(m)) mit dem Netzwerk-Service-Provider (11) eine Kommunikationssitzung aufbaut und von diesem eine Identifizierung von einem weiteren Namen-Server empfängt.

17. Computerprogramm-Produkt nach einem der Ansprüche 13 bis 16, welches ferner ein Namen-Server-Abfragesteuerungsmodul aufweist, welches veranlaßt, daß die externe Vorrichtung (12(m)) eine Liste von Namen-Servern erhält, welche der externen Vorrichtung (12(m)) identifiziert wurden, und die Namen-Server in der Liste nacheinander in Reaktion auf eine Anfrage zum Zugriff auf eine andere Vorrichtung abfragt, wobei die Anfrage eine Sekundäradresse der anderen Vorrichtung enthält, solange bis die externe Vorrichtung (12(m)) eine Netzwerkadresse empfängt, und wobei die externe Vorrichtung (12(m)) in jedem Abfragevor-

gang eine Netzwerkadressen-Anfragesnachricht zur Übertragung über das Netzwerk (14) erzeugt, welche durch einen der Namen-Server in der Liste zu beantworten ist, und von diesem eine Netzwerkadressen-  
Antwortnachricht empfängt.

18. Computerprogramm-Produkt nach einem der An-  
sprüche 13 bis 17, bei welchem die Verbindung zwi-  
schen der externen Vorrichtung (12(m)) und der Fire-  
wall (30) ein Sicherheitstunnel ist, in welchem wenig-  
stens ein Abschnitt der zwischen der externen Vorrich-  
tung (12(m)) und der Firewall (30) übertragenen Nach-  
richten verschlüsselt ist.

Hierzu 1 Seite(n) Zeichnungen

5

10

15

20

25

30

35

40

45

50

55

60

65

